

SUMMARY

So far, the Commission has failed to fulfill its responsibility under CALEA to protect the privacy of the American people. While acknowledging that Congress intended to balance privacy and law enforcement interests, on all the issues that matter most to privacy, the Commission so far has rejected privacy concerns and accepted law enforcement's broad reading of the Act. The one exception is packet switching, where the Commission has not ruled one way or the other.

On an issue of vital concern to the privacy of the more than 50 million users of wireless phones, the Commission has ignored the plain words of the statute in tentatively finding that wireless phone location information is a CALEA mandate. The provision of the Act on which the Commission relies -- the definition of "call-identifying information" -- simply does not include the word "location." Each of the terms in the definition of call-identifying information has a precise meaning separate from location. Departing from the plain words of the Act, the Commission instead finds a mandate for location information implied in a separate provision, one that actually is a prohibition against providing location information as part of call-identifying information under a pen register order. Before concluding that this prohibition implies a mandate, the Commission would have to look to the legislative history to clear up any ambiguity. The Committee reports are 100% clear that location information is not required as part of call-identifying information.

In terms of packet switching, CDT believes that there is a way, consistent with the evolving packet technology, to meet law enforcement's needs for signaling information while preserving the Constitutionally-based distinction between signaling and content in the wiretap laws. Our proposal is that a carrier, when presented with a pen register or trap and trace order,

should disclose to the government the signaling information that such carrier uses for call processing purposes. Packet technology allows any service provider in the network to distinguish the signaling information that it uses, and to separate it from what it treats as content. The increasing deployment of packet technologies in the public switched telephone network, as well as the increasing use of the Internet for voice telephony, raise questions for the conduct of electronic surveillance. We believe that these questions can be answered in the context of CALEA, without sacrificing either privacy or the interests of law enforcement, and without requiring extensive reengineering of packet technology.

TABLE OF CONTENTS

SUMMARY	i
INTRODUCTION	1
I. LOCATION INFORMATION IS NOT A CALEA MANDATE	4
A. The Plain Words of the Statute Do Not Include “Location”	5
B. The Commission’s Reading is Actually Inconsistent with the Standard	7
C. It Is The Congress, Within The Bounds Of The Constitution, That Sets the Framework for Protecting Privacy, Not Carriers And The FBI	8
D. The Language of Section 103(a)(2) Prohibits Location as Part of Call-Identifying Information; It Is Not Surplusage nor Can It Be Read as a Mandate for Location Information	9
E. The Legislative History Clearly Excludes Location Information from the Definition of Call-Identifying Information	11
F. The Location of Wireless Phones Is More Personally Revealing Than the Location of Wireline Phones	12
II. CALEA REQUIRES CARRIERS TO DISTINGUISH BETWEEN CALL- IDENTIFYING DATA AND CALL CONTENT IN PACKET SWITCHING ENVIRONMENTS, AS THEY DO IN CIRCUIT SWITCHED ENVIRONMENTS, BASED ON WHAT INFORMATION A CARRIER USES TO ROUTE COMMUNICATIONS	13
A. Overview	13
1. Background: The Distinction Between Content And Signaling Information In The Surveillance Laws Is Constitutionally-Based	14
2. CALEA Was Intended To Track And Preserve The Surveillance Laws’ Distinction Between Content And Signaling Information	14
3. CDT’s Privacy Proposal Offers A Consistent, Rational Approach To Preserving In Packet Environments The Heightened Privacy Protection Accorded To Communications Content, Without Altering The Technology And Without Denying Law Enforcement What It Needs	15
4. TIA Has Misconstrued CDT’s Position	17

5.	Many Current and Projected Applications of Packet Data Are Not Covered by CALEA in the First Place	20
6.	Law Enforcement Needs Can Be Met and Privacy Can Be Preserved Consistent with Network Design	21
B.	In Communications Networks, The Distinction Between Call-Identifying Information And Call Content Is Relative	21
1.	The Open System Interconnection (“OSI”) Reference Model Is Based on the Seven Layer Protocol Stack	22
2.	Call-Identifying Information and Content Are Relative Concepts, Depending On The Carrier That Is the Subject Of An Order	23
3.	The OSI Reference Model Applied to Telephony	24
C.	A Service Provider Specific Interpretation Of Call-Identifying Information Is Consistent With The CALEA’s Plain Language And Legislative Intent	25
1.	The Definition of “Call-Identifying Information” Includes “Direction” ...	25
2.	Carriers Are Only Required To Provide Call-Identifying Information That Is “Reasonably Available”	26
3.	The Legislative History Shows That Congress Looked at Call-Identifying Information from the Perspective of the Carrier	27
D.	With A Subjective Standard, Capturing And Separating Routing Information Are Feasible	29
CONCLUSION.....		31

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

RECEIVED

DEC 14 1998

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of)	
)	
Communications Assistance)	CC Docket No. 97-213
For Law Enforcement Act)	

**COMMENTS OF THE
CENTER FOR DEMOCRACY AND TECHNOLOGY**

Pursuant to the Further Notice of Proposed Rulemaking in the captioned docket (FCC 98-282, rel. Nov. 5, 1998)(the "*Further Notice*"), the Center for Democracy and Technology ("CDT") hereby submits these comments on the implementation of the Communications Assistance for Law Enforcement Act (the "Act" or "CALEA")¹ in order to address issues raised by the Commission in connection with wireless location information, packet-mode communications, and the FBI punch list.

INTRODUCTION

So far, the Commission has failed to fulfill its responsibility under CALEA to protect the privacy of the American people. While it has acknowledged that Congress intended to balance privacy and law enforcement interests, so far on all the issues that matter most to privacy, the Commission has rejected privacy concerns and has accepted the law enforcement position. The one exception is packet switching, where the Commission has not ruled one way or the other.

¹ Public Law No. 103-414, codified at 47 U.S.C. §§ 1001-1010 and in various sections of Title 18 and Title 47.

In giving inadequate weight to privacy, the Commission seems to have assumed that the wiretap laws other than CALEA and the decisions of the courts will afford adequate privacy protection. However, such an assumption finds no support in CALEA itself, which mandates privacy protections apart from and in addition to those found elsewhere. CALEA recognizes that the wiretap laws by themselves no longer provide a sufficient privacy backstop because communications technology is changing so rapidly, so much information is being transmitted in electronic form, and people have so woven wireless phones, the Internet and other new services into their daily, personal lives. Consequently, privacy protection must be a design criterion. In this next phase of the proceeding, the Commission needs to reset its sights on the fundamental balance represented by CALEA: the Act requires telecommunications systems to be designed with privacy protection as a requirement as important as law enforcement surveillance.

The Commission's tentative conclusion in the *Further Notice* that location information is a CALEA mandate is particularly startling because it represents such a sharp repudiation of one of the key compromises struck in 1994 when CALEA was being debated and drafted. At the time, CALEA represented a huge departure: law enforcement interests for the first time were being imposed on the design of the nation's telecommunications system, with tremendous risk to privacy. Those of us at CDT who participated in the debate from a privacy perspective believed then that we had reached a compromise through the legislative process that balanced the interests of law enforcement, privacy and industry, a compromise that imposed both substantive and procedural limits on law enforcement's requirements. That compromise is reflected both in the language of CALEA and repeatedly throughout its legislative history.

One element of that compromise in 1994 was the FBI's concession that wireless phones

would not be required to provide location of any kind. The FBI has since decided to repudiate that deal, and the Commission has tentatively agreed. To do so, the Commission has taken the statute's prohibition against providing location information as part of call-identifying information under CALEA and transformed it into a mandate to provide location information. The Commission has allowed the FBI's desire for maximum surveillance capability to trump the plain words of the statute and the unambiguous legislative history. It has accepted an industry-FBI compromise on location information, when Congress had already determined that location information should be excluded from CALEA's mandate. If the Commission's tentative decision stands, it will send a powerful signal that the Commission cannot be relied upon to enforce the kind of balancing CALEA requires between the law enforcement claims of the FBI and the public's right to communications privacy.

In terms of packet switching, we start from two principles: that CALEA was intended to operate within the privacy framework of the wiretap laws, and that CALEA was not intended to require fundamental departures from the direction in which telecommunications technology is evolving. One of the central privacy principles of the wiretap laws is the sharp distinction between signaling information and the content of communications. One of the central technological directions of telephony is the incorporation of packet technology. We believe that, under CALEA, it is not necessary for either one of these factors to cancel out the other. CDT believes that there is a way, consistent with the evolving packet technology, to meet law enforcement's needs for signaling information while preserving the basic distinction between signaling and content in the wiretap laws. Our proposal is that a carrier, when presented with a pen register or trap and trace order, should disclose to the government the signaling information

that such carrier uses for call processing purposes. Packet technology allows any carrier in the network to distinguish the signaling information that it uses and to separate it from what that carrier treats as content. Neither the technology nor the statute requires a carrier to read through layers of signaling information to do so.

On the additional capabilities sought by the FBI (the so-called "punch list"), CDT is in agreement with industry. Our views were made clear in our May 20, 1998 and June 12, 1998 filings, in which we explained why none of the punch list items is required by the statute and why several of them have serious privacy implications. We will make more extensive comments in our reply, informed by the comments of industry and the DOJ/FBI. For the purpose of this filing, we focus on those two issues (location information and packet switching) where we believe that industry erred in agreeing with the DOJ/FBI, with the gravest implications for privacy. We also note that the approach we outline here for dealing with packet switching -- to focus on signaling information used by a carrier or service provider for call processing and not on data used by another carrier -- also supports our position on post cut-through dialed digits, one of the punch list items.

DISCUSSION

I. LOCATION INFORMATION IS NOT A CALEA MANDATE

In proposing to accept the FBI's claim that some type of location information is a CALEA mandate, the Commission is on the verge of setting a terrible precedent. The Commission, faced with the complaint that wireless phones will be turned into tracking devices, hopes to avoid the implications of its decision by limiting the requirement to provide cell site location to the beginning and end of a call. Yet there is no basis in the language of CALEA for

this kind of line-drawing. Either location information is a CALEA mandate or it is not. Inevitably, if it finally concludes in this proceeding that location information is required by CALEA, the Commission will find itself boxed-in in the near future when more precise location information becomes available in wireless systems. At that point, having proceeded down this road, the Commission will have no choice but to conclude that such more precise information must then be included as an item in the CALEA surveillance interface. The privacy implications for tens of millions of wireless phone users are truly chilling.

A. The Plain Words of the Statute Do Not Include “Location”

The Commission claims to have adhered to the plain words of the statute, but it clearly has not done so in reading a location requirement into CALEA. Simply reading the plain words of the Act, the definition of “call-identifying information” does not include the location of wireline or wireless phones.

Call-identifying information is defined as information identifying the “origin, direction, destination or termination” of a communication. The word “location” is simply not there. Each of the four terms of the definition has a meaning independent of location. The only way that the Commission could possibly interpret the definition of call-identifying information as including location is to read one or more of the those terms as meaning *both* phone number information for either the calling or called party *and* information identifying the cell site.

The terms on which the Commission rests its case are “origin” and “destination.”² Yet these words have obvious meanings apart from location: “origin” means the phone number of

² One sign of the problems with the Commission’s reading of the statute is that the Commission interprets the word “destination” differently than the J-STD. The J-STD states:

the calling party, while “destination” means the number of the called party on an outgoing call. It was obviously the intent of Congress to impose the same obligations on wireline and wireless carriers. Yet the *Further Notice* interprets “origin” and “destination” as meaning more in the case of wireless carriers than it means in the case of wireline carriers. In wireless systems, the Commission would have these words mean not only the number of the calling and called parties, respectively, but also the cell site of one or the other. This violates a fundamental rule of statutory interpretation: each word in a statute should be given a single and unique meaning. Under the *Further Notice*, the words of the call-identifying definition are given different meanings in different situations.

There is another problem with the Commission’s theory: it fails to support the Commission’s view that CALEA requires cell site identification *at the end of calls*. Certainly, a call only has one point of “origin,” so in the case where the wireless intercept subject is the calling party, there can be no statutory requirement, even under the Commission’s reading of the words of the Act, for cell site location at the end of the call. (The word “termination” clearly doesn’t apply, since it refers to the answering party.) This is just another illustration of how the plain words of the statute do not support the Commission’s interpretation.

As interpreted by this Standard: **destination** is the number of the party to which a call is being made (e.g., called party); **direction** is the number to which a call is re-directed or the number from which it came, either incoming or outgoing (e.g., redirected-to party or redirected-from party); **origin** is the number of the party initiating a call (e.g., calling party); and **termination** is the number of the party ultimately receiving a call (e.g., answering party).

See J-STD at 5. (emphasis in original). Thus, under the standard, destination means the number of the called party on an outgoing call, which could never include location. Under the J-STD, “termination” refers to the answering party, so it is “termination” that would include location if the Commission’s reading were correct. Of course, it is clear from the above definition that the drafters of the J-STD did not believe that location was included in “call-identifying information” at all.

B. The Commission's Reading is Actually Inconsistent with the Standard

The *Further Notice* states that “origin” and “destination” include location, but the J-STD includes location only of the intercept subject. From a privacy perspective, this is better than requiring location information also of those calling or called by the intercept subject, but it shows that the J-STD was based on expediency – the desire of the carriers to achieve a compromise with the FBI – rather than the mandates of the Act. It highlights as well the flaws in the Commission's interpretation. Consider the following scenario: the intercept subject is the called party, and the calling party is wireless. CALEA and the J-STD clearly require the intercept subject's carrier to identify the “origin” of the call, by providing the telephone number of the calling party. Now if the word “origin” also meant location, as the Commission says that it does, the intercept subject's carrier would logically have to provide the cell site of the calling party. This might be technically feasible – every wireless call could include some sort of cell indicator that was passed on to the called party's carrier – and it has an obvious utility to law enforcement, but the J-STD does not require it. Why does “origin” not include location when the calling party is not the intercept subject, although it includes the calling party's phone number? The distinction has no basis in the Act; it came about because the carriers, in their compromise with the FBI, did not agree to it.

The same inconsistency applies in the case where the calling party is the intercept subject and the called party is wireless. CALEA and the J-STD clearly require the intercept subject's carrier to identify the “destination” of the call, by providing the called party's phone number. But if “destination” also includes location, as the Commission has tentatively concluded it does, the intercept subject's carrier would have to include the location of the called party. That is

obviously impossible, and the J-STD does not require it, but under the Commission's reading, it would be a mandate, to be excused only because it was not reasonably available.

These inconsistencies highlight the illogic of the Commission's interpretation.

C. It Is The Congress, Within The Bounds Of The Constitution, That Sets the Framework for Protecting Privacy, Not Carriers And The FBI

The *Further Notice* recognizes that the inclusion of location information in the J-STD was the result of a compromise between industry and the FBI: The industry participants concluded that location information was not required, but they included it anyway in an effort to reach agreement with the FBI. (The FBI responded to this and other industry concessions by filing a deficiency petition at the Commission.) In the Commission's view, the fact that industry agreed to provide location information legitimizes the inclusion of the capability.

This is not the way CALEA was intended to work. The FBI and industry are not free to compromise away the privacy of citizens. It was up to Congress to strike the compromises, and one of them was that location information would not be included. It is now the responsibility of the Commission to enforce that CALEA mandate in the standard it establishes under Section 107(b) of the Act.

Either location is a mandate or it is not. Obviously, the J-STD, which the Commission seeks to uphold on this point, does not treat location as a CALEA mandate, because it picks and chooses when to provide location information. The Commission should come to the same conclusion, and declare as a matter of statutory interpretation that location information is not a mandate. This will establish an important precedent that will save carriers from being forced into future compromises with the FBI as it presses for more and more precise location information.

D. The Language of Section 103(a)(2) Prohibits Location as Part of Call-Identifying Information; It Is Not Surplusage nor Can It Be Read as a Mandate for Location Information

Notwithstanding its decision that CALEA should not mandate location information, Congress recognized that some wireless systems already generate location information and would continue to do so, apart from CALEA.³ If such information was generated, Congress knew that it could be turned over to law enforcement as transactional data, and Congress was worried that carriers would turn it over pursuant to a pen register order as part of the call-identifying information. While Congress did not want to preclude carriers from disclosing location information, it was eager to make it clear, as one of the privacy enhancements it included in CALEA, that carriers could not provide location information along with mandatory call-identifying information under a mere pen register order.

To make it clear that location information could not be provided under a pen register order as part of call-identifying information, Congress added the following language to CALEA:

except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of title 18, United States Code), such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent the physical location may be determined from the phone number);⁴

³ H.R. Rep. No. 103-827, pt. 1, at 17 (1994) ("House Report"). The Senate Judiciary Committee report is identical to the House Report being cited. S. Rep. No. 103-402 (1994). No other committees filed reports. Thus, although some sections of the legislation changed after the Judiciary Committees acted, the Judiciary Committee reports remain the best legislative history. Many provisions ultimately enacted were unchanged from the version reported by these Committees.

⁴ CALEA, § 103(a)(2).

With this language, Congress sought to ensure that carriers would not include location information with call-identifying information, since call-identifying information would be provided under a pen register or trap and trace order, under a standard that Congress felt was too low for location information.

Ironically, the Commission has turned this CALEA imperative on its head, ignoring this straightforward prohibition against providing location information as part of the call-identifying information acquired under a pen register order. Somehow, the Commission has interpreted the statutory prohibition as a mandate to *include* location as part of call-identifying information. Yet Congress could not have been clearer.

Section 103(a)(2) is not surplusage. Central to understanding how CALEA works is the difference between what is mandated by CALEA and what carriers can otherwise be compelled to disclose to law enforcement if they happen to have it in their systems. Congress saw that, even if CALEA did not mandate location information, it would be available in some systems. Section 103(a)(2) says that if carriers have location information and provide it to law enforcement, they cannot provide it under the pen register as part of call-identifying information. Congress did not specify how the government could compel production of location information, it just made it clear that the standard had to be stronger than a pen register order. (The Justice Department has since concluded that the authority of 18 U.S.C. 2703(d) is appropriate.) This was intended as a modest enhancement in privacy, but the Commission would turn it into a location information mandate. It is especially illogical for the Commission to conclude that Congress, while signaling its concern with location information by prohibiting carriers from

providing it under a pen register, simultaneously would have required them to build a location capability and make it available under some other, unspecified standard.⁵

E. The Legislative History Clearly Excludes Location Information from the Definition of Call-Identifying Information

Even under the Commission's reading, the reference to location information in Section 103(a)(2) cannot, standing alone, be read as a mandate. Section 103(a)(2) says what carriers cannot do, it does not say what they shall do. The Commission has read the reference to location information in 103(a)(2) as implying that location was included in the definition of call-identifying information, but the most that the Commission can get from Section 103(a)(2) is an *implication* of a requirement.

If there is an ambiguity on this point, the Commission must look to the legislative history. The Committee reports clear up any ambiguity. The reports of both the House and Senate Judiciary Committees state that:

[CALEA requires carriers to] isolate expeditiously information identifying the originating and destination number of targeted communications, but not the physical location of targets.⁶

⁵ In their reports, the Committees, in discussing Section 103(a)(2), described it as one of the features that "add protections to the exercise of the government's current surveillance authority." The reports state that the bill:

Expressly provides that the authority for pen registers and trap and trace devices cannot be used to obtain tracking or location information, other than that which can be determined from the phone number. Currently, in some cellular systems, transactional data that could be obtained by a pen register may include location information.

House Report at 17. This shows that the Committees viewed the reference to location information in section 103(a)(2) as a response to a current problem, a problem existing in systems before CALEA was enacted and took effect. Congress would not have been concerned with limiting governmental access to location information "currently" available "in some cellular systems" if it was at the same time requiring all cellular systems to provide location information.

⁶ House Report at 17.

The reports go on to make it clear that “call-identifying information” is limited to dialed number information:

For voice communications [call-identifying information] is typically the electronic pulses, audio tones, or signalling messages that identify the numbers dialed or otherwise transmitted for the purpose of routing calls through the telecommunications carrier’s network. In pen register investigations, these pulses, tones, or messages identify the numbers dialed from the facility that is the subject of the court order or other lawful authorization. In trap and trace investigations, these are the incoming pulses, tones or messages which identify the originating number of the facility from which the call was placed. . . .⁷

F. The Location of Wireless Phones Is More Personally Revealing Than the Location of Wireline Phones

There are grave privacy interests at stake here. The FBI and the Commission in the *Further Notice* try to argue that cell site location is comparable to what is available in wireline systems, but wireless phone location is far more personally revealing than wireline location. Wireless phone users carry their phones with them: an individual user is more closely associated with a wireless phone than with that person’s wireline phone. When a call is made on a wireline phone, it means that somebody is at the location, but it is not apparent who. When a call is made on a wireless phone, it almost always is the individual subscriber. In this way, wireless phone location information is far more revealing than the fact that a street address is associated with a wireline phone number. Treating the two alike, as the Commission’s reasoning would permit, is flatly inconsistent with CALEA’s mandate.

⁷ *Id.* at 21.

II. CALEA REQUIRES CARRIERS TO DISTINGUISH BETWEEN CALL-IDENTIFYING DATA AND CALL CONTENT IN PACKET SWITCHING ENVIRONMENTS, AS THEY DO IN CIRCUIT SWITCHED ENVIRONMENTS, BASED ON WHAT INFORMATION A CARRIER USES TO ROUTE COMMUNICATIONS

A. Overview

The interim industry standard developed in response to CALEA radically decreases privacy protection by permitting carriers to disclose to the government the contents of a person's packet mode communications when the government does not have the authority to intercept them. This is not necessary to serve the needs of law enforcement, nor is it technologically necessary. The technology of packet switching allows a carrier to provide to a government agency everything it is entitled to intercept, without compromising the privacy of communications that the government is not authorized to intercept.

The CDT proposal is simple: any carrier using packet technologies should disclose pursuant to a pen register order the transactional information *that it uses* to process communications. A carrier may (but need not) disclose the transactional information used by other carriers, but it should not disclose content. The technology allows a carrier to readily distinguish between the transactional data that it uses for routing and the rest of a packet. Standard system maintenance features and readily available packet-sniffing programs allow systems operators to identify and isolate the call routing information used by their systems.

Distinguishing in this way between routing information and content does not mean that law enforcement agencies have to traverse the length and breadth of the PSTN or the Internet to collect the information they need. Much of the routing or signaling information in a packet network is of no interest to law enforcement and most of the nodes in a network are inefficient places for law enforcement to conduct surveillance. Law enforcement agencies will continue to

be able to obtain the information they are interested in by going to the local exchange carriers, ISPs, and the providers of leased lines and private networks.⁸

1. Background: The Distinction Between Content And Signaling Information In The Surveillance Laws Is Constitutionally-Based

The wiretap laws have always drawn a distinction between the content of a communication and the dialing or other signaling data used by a carrier to route communications. The Supreme Court has held that the content of electronic communications is constitutionally protected by the privacy provisions of the Fourth Amendment, requiring a high level of justification and judicial approval to intercept, while there is no constitutionally-protected privacy interest in signaling data. Congress has protected signaling data by statute (the pen register law), but the standard for interception is very low. Call content interception is supposed to be an investigative means of last resort; interception of signaling data has become a technique of first resort in many cases. Law enforcement conducts at least ten times as many interceptions of signaling data as it does of content.

2. CALEA Was Intended To Track And Preserve The Surveillance Laws' Distinction Between Content And Signaling Information

CALEA preserves this distinction and reinforces it, using the term "call-identifying information" to describe signaling information and requiring carriers to protect the privacy of communications not authorized to be intercepted. It would represent a de facto gutting of the surveillance laws if the introduction of packet switching meant that law enforcement agencies were to receive content they were not authorized to intercept. Some have characterized CDT's

⁸ ISPs, leased lines and private networks are not covered by CALEA, but have an obligation to cooperate with law enforcement surveillance under 18 U.S.C. § 2518(4).

concerns as presenting a Hobson's choice: to meet law enforcement's needs, carriers either must provide the entire data stream or undergo expensive reengineering of their systems to be able to read through layers of signaling information. In fact, there is a third option, one that is consistent with the technology, gives law enforcement what it needs, and preserves the privacy distinctions inherent in the wiretap laws.

3. CDT's Privacy Proposal Offers A Consistent, Rational Approach To Preserving In Packet Environments The Heightened Privacy Protection Accorded To Communications Content, Without Altering The Technology And Without Denying Law Enforcement What It Needs

CDT has argued that CALEA requires carriers using packet switching technologies to recognize the distinction between content and signaling data: when presented only with an order for call-identifying information, carriers should provide only signaling data, not content.

This raises the question: what signaling data? CDT's answer is that any carrier or service provider can only be expected to provide what it treats as signaling data. No carrier has the obligation to peel back protocol layers or open envelopes to understand the full stack of signaling data.⁹ It is up to law enforcement to figure out what it really wants as addressing information and go to the carrier or service provider that "reads" that layer. Then it is a separate question whether that service provider can isolate just the signaling information that law enforcement wants or copy only the addressing information at that layer, but certainly that is a far less daunting

⁹ We explain the layered model of signaling information below in Section II.B, p. 21 et seq. We are not concerned at this point that some signaling data provided by a carrier may be irrelevant to law enforcement or that some may be more revealing than routing data for a telephone call. CDT is not arguing that carriers presented with a pen register order need to draw distinctions within the layers of routing information or to withhold some routing information. All CDT is arguing is that carriers should find a way to withhold content from law enforcement. It is a separate concern (one not before the FCC) that the signaling data in packet environments is richer than the signaling data in POTS.

exercise than analyzing all the layers. We believe that the technology is available to accomplish that more focused task.

What signaling data does the government want in a packet environment? Much of the signaling data in a packet network is of no interest to law enforcement. Usually, what law enforcement will want is information identifying the sender and the intended recipient of a message. In many cases this will be an Internet address. Law enforcement should go to the service provider that is in the best position to give it this information.

This is no different from what the government already does today. For example, the government does not conduct ordinary telephone surveillance by going to interexchange carriers or other large pipelines -- it goes to the local exchange carrier. On the other hand, the government by and large does not intercept email from the local exchange carrier -- it goes to the ISP or on-line service provider (*e.g.*, America Online), where it captures messages while they are in a store and forward mode. The government does not ask the LEC to read the to and from lines on email -- the government goes to the ISP or on-line service provider to get that information.

To learn who is communicating with whom in the packet context, where is the best place for the government to go? In the case of individuals, this will be the ISP or on-line service. This means that law enforcement will go to the LEC for dialing information and to the ISP or other on-line provider for packet signaling information. This imposes no unique obligation on law enforcement. Given telecommunications competition and given the diversity of telecommunications services now available to users, law enforcement already must go to

different service providers for different information.¹⁰ As Congress clearly stated “CALEA is not intended to guarantee one-stop shopping for law enforcement.”¹¹

CDT’s approach offers the Commission the only consistent way to treat both post cut-through dialed digits and packet switching. CDT agrees with the carriers that they should not be required to reach into their content channels and extract digits dialed after call cut-through. A LEC treats post cut-through dialed digits as content. If the government wants post cut-through dialed digits, it should either get a content interception order, or go to the carrier that treats the post cut-through dialed digits as signaling. In the same way, a LEC handling a dial up access call to an ISP treats everything after call cut-through as content. If the government wants the email signaling information sent to the ISP, it should obtain a content order or go to the ISP, which treats that post cut-through signaling information as signaling information.

4. TIA Has Misconstrued CDT’s Position

To date, the reply comments filed by the Telecommunications Industry Association last June are the most extensive comments on the packet issue. CDT largely agrees with TIA’s factual description of the protocol stack employed in assembling and addressing packets, but we disagree with TIA’s conclusions, largely because TIA seems to have misunderstood our position; we are not asking any particular carrier to analyze or segregate data at higher levels of a protocol stack than those which the carrier must already process in order to route the packet.

¹⁰ A target may use one carrier for his wireless service, one for wireline service at home, a third carrier at his office, a fourth one for his pager. A person seeking to avoid surveillance may use multiple wireless carriers or have multiple phones and multiple accounts. There is no way to undo this. The Commission is not obliged to apply, nor should it apply a one-stop model to the consequences of competition.

¹¹ House Report at 23.

For example, TIA states:

In a layered protocol, each layer views the layer above it as content. The content for the current layer, plus its routing information (the header), becomes the content portion for the next lower layer. . . .

A telecommunications carrier transporting packet data is often responsible for providing hardware and software support only for the physical layer, and does not have any reason to segregate higher-layer content from higher-layer routing information.¹²

CDT agrees with both these statements and finds neither inconsistent with its proposal. Indeed, they support CDT's position: a carrier that supports only the physical layer (layer 1 in a protocol stack) need only provide law enforcement with physical layer routing information. If the carrier treats everything else "above" the physical layer as content, it is not required to provide those higher layers under a pen register order.

However, TIA goes on to state:

To extract packet data routing information, two basic steps must be completed. First, packets of interest must be identified and captured. Identification of particular data packets for the purpose of extracting call-identifying information presents technical challenges that most carriers are not currently capable of meeting. In a stream of bits riding across a circuit, the system must be able to recognize the correct sequence of bits which delineates the start of a data packet. This can require that the system "watch" all circuits all the time, looking for data packets. For example, with respect to the X.25 protocol, CDT is correct that communications "are connection-oriented [and] contain separate and distinct call set-up and teardown messages." However, this does not mean that separate provision of only the set-up and teardown messages is "reasonably available," as CDT suggests. A carrier that provides only physical layer transport for an X.25 network would have no reason or ability to detect and segregate such messages.¹³

¹² TIA Reply Comments at 13-15.

¹³ *Id.* at 15.

In a situation like the one TIA describes, the surveillance problems are much deeper than those posed by CDT's proposal. If carriers cannot "look for data packets," then they cannot comply with the requirements of CALEA section 103(a)(1) and (2) to isolate content, let alone the requirement of Section 103(a)(4) to distinguish between content and call-identifying data. The simple answer in a situation like the one described by TIA's scenario is that (1) law enforcement should not be going to this point in the network for surveillance assistance; and (2) CALEA does not cover the situation that TIA seems to be describing, since CALEA does not cover a carrier "that merely interconnects two other carriers."¹⁴

TIA goes on to assume that CDT is proposing that carriers be required to "extract" routing information by going through the protocol layers. TIA states:

Second, once packets have been captured, the relevant information must be extracted. The process of extracting header information from content in a layered protocol stack is very complex. To obtain routing information at a level which would provide relevant "call-identifying information" to law enforcement, a carrier would need to extract headers up to at least layer 3+. The system would first strip off routing information (headers) from layer 1 to get to the content. That content contains the header and content for layer 2, which must be separated. Then that content contains the header and content for layer 3, and so on. At each layer the system must not only recognize the beginning and end of each packet, but must recognize the protocol being used so that it can separate the header from the content.¹⁵

This is not CDT's position. Contrary to TIA's assumption, CDT is not arguing that CALEA imposes an obligation to strip off layers or conduct any analysis of anything that the carrier's system views as content.

¹⁴ House Report at 23.

¹⁵ TIA Reply Comments at 16.

5. Many Current and Projected Applications of Packet Data Are Not Covered by CALEA in the First Place

The Commission should recognize that many services that use packet switching are not covered by CALEA in the first place, given the Act's exclusion of information services, of private networks, and of interexchange carriers.

For now, CDT believes that the Commission would do well to broadly interpret the information services exemption. Implementing CALEA in POTS is difficult enough without extending the Act's reach into Internet-based services. For this reason, the Commission should exclude from this CALEA rulemaking all telephony over the Internet. In this proceeding, the Commission should focus on packet technologies in the PSTN. That is where law enforcement conducts the bulk of its surveillance.¹⁶

Even in the PSTN, packet protocols appear largely in contexts excluded from CALEA. Private networks are excluded.¹⁷ Interexchange carriers are excluded, as are any carriers connecting other service providers.¹⁸

With all of these exclusions, it is incumbent on those who drafted the standard to explain where packet technologies will be encountered by law enforcement seeking surveillance access, other than those situations we have described here. As of now, we know of no uses of packet technology covered by CALEA that do not fit the model we have proposed.

¹⁶ "The only entities required to comply with functional requirements are telecommunications common carriers, the components of the public switched network where law enforcement agencies have always served most of their surveillance orders." House Report at 18.

¹⁷ See CALEA, § 103(b)(2)(B).

¹⁸ *Id.* Although excluded, interexchange carriers and other carriers connecting service providers are obliged to cooperate with law enforcement surveillance requests under 18 U.S.C. 2518(4) and 3124.

6. Law Enforcement Needs Can Be Met and Privacy Can Be Preserved Consistent with Network Design

The emergence of packet-switching in telephony does not require carriers to abandon their responsibility to protect the privacy of communications not authorized to be intercepted:

- What is call-identifying information in a packet-switched context?

Call identifying information is relative to the task of the carrier on which the surveillance order is served. Such an outcome inevitably flows from the effects of competition and technological change on the telecommunications network. There is no longer one signaling protocol. There is no longer one type of service provider. A service provider, when served with a call-identifying intercept order, can only be required to provide what it treats as call-identifying information. It cannot be required to provide to law enforcement what somebody else treats as call-identifying information.

- Can carriers be expected to separate call identifying data from content in packet switched environments?

Yes, in some if not all environments, carriers can and therefore must distinguish content from call-identifying data. This distinction can be found in many if not all packet protocols. It has been suggested that it is too hard in a packet switched system to distinguish between call-identifying information and content. CDT believes this is not true. At every stage of a packet's path, it is possible to draw a line between call-identifying information and content. Where that line is drawn will shift from carrier to carrier and from point to point in the network, but wherever law enforcement serves its order, the service provider can make the distinction, and should be required to do so whenever it is reasonably achievable.

B. In Communications Networks, The Distinction Between Call-Identifying Information And Call Content Is Relative

The distinction between call-identifying information and content exists in both circuit switched and packet switched environments. In both types of networks, the distinction is relative. In circuit switched systems, when the subscriber uses a LEC to dial 1 800 CALL ATT, the LEC treats that as signaling information. Everything after call cut-through is content from the perspective of the LEC. But the post cut-through dialed digits are call-identifying information from the perspective of the long distance carrier. Similarly when a subscriber dials

into an ISP, the local access number for the ISP is call-identifying information for the LEC. Everything after that is content from the perspective of the LEC, even though the call may last for hours and involve multiple emails plus “visits” to numerous websites. It is impossible for the LEC to extract post cut-through signaling information. But if the government goes to the ISP, it can and does receive the email address, IP addresses and other information that is treated by the ISP as signaling.

This same principle applies in the packet environment. As a packet network manipulates information that is transiting its connections, each component of the network has a specific perspective as to what is content and what is call-identifying information. This perspective is dependent upon where in the network the information is being manipulated.

1. The Open System Interconnection (“OSI”) Reference Model Is Based on the Seven Layer Protocol Stack

At this point, it is probably necessary to describe only briefly the basics of packet network architecture. We do not believe there will be any significant disagreement over the architecture itself, only over the consequences for law enforcement surveillance.

The Open System Interconnection (OSI) reference model provides a model of communications architecture by which packet data protocols are described. In the OSI model, the problem of communicating among diverse networks of computers is divided into seven reasonably discrete and self-contained sub-tasks.¹⁹ Since these sub-tasks are organized hierarchically, they are referred to as layers. Different layers or combinations of layers may have

¹⁹ Not only does dividing the problem into discrete sub-tasks promote interoperability, it also permits innovation and competition to thrive. Since each of these sub-tasks is self-contained, it is easy to change one without affecting the others. This has made rapid development and innovation much easier.

their own protocols. Protocols are standardized means for transmitting data; when layered they are frequently referred to as “protocol stacks.” The “lowest” layer (Layer 1) is the physical layer; the “highest” layer (Layer 7) is the application layer. Layer 3 is the network layer.

In the OSI reference model, for data to pass from one computer’s application (such as a Web browser) to a second computer’s application (such as a Web server), the data must pass down through the layers of the originating system to the physical layer where the data is transferred to the receiving system. Once at the physical layer of the receiving system, the data passes up through the layers of the second system until it reaches its final destination at the recipient application.

2. Call-Identifying Information and Content Are Relative Concepts, Depending On The Carrier That Is the Subject Of An Order

As a message packet is created, some information or control data is added at each layer. This control data consists of routing or signaling information, as well as other sorts of information. As a segment of content passes through the layers of the protocol stack, new control data is added, in the form of a prefix (or header), to whatever is passed down from the layer above. Each succeeding layer treats the information from the layers above, including the headers added by the layers above, as content.

In a packet switched network, it is likely that a message will have to travel through several different computers (or nodes) before it reaches its final destination. A message that passes through an intermediate node does not have to be processed by the intermediate node’s complete protocol stack. When an intermediate node receives a message, the message will only rise through the stack to the layer necessary to forward it on its way. Since intermediate nodes

do not (and often cannot) process a message above a certain layer, whatever is above that layer must be viewed as content.

In this respect, the concepts of signaling data and content are relative, dependent upon the perspective of the layer manipulating the packet. Thus, CDT agrees with the factual statement by TIA that, “In a layered protocol, each layer views the layer above it as content.”²⁰ However, we believe that the conclusions TIA draws from this are wrong.

3. The OSI Reference Model Applied to Telephony

TIA argues, correctly, that a “telecommunications carrier transporting packet data is often responsible for providing hardware and software support only for the physical layer”.²¹ As far as that carrier is concerned, only the header information for layer 1 (the physical layer) can be considered call-identifying information. All the other information contained in the packet must be considered content, from the perspective of that carrier. In other cases, the telecommunications carrier might be responsible for higher layers of the protocol stack. In an Integrated Services Digital Network (“ISDN”), the carrier might be providing service up through layer 3, the network layer. If so, then the header information for layers 1-3 should be considered call-identifying information from the perspective of the carrier. Layer 4 and above would be content.

More sophisticated concepts like tunneling and Virtual Private Networks (“VPNs”) are based on the same principles. In tunneling, one network can send information via another network by encapsulating its data link layer within the data link layer of another protocol. While

²⁰ TIA Reply Comments at 13.

the modified packet is traveling on the intermediate network, what lies above the data link layer is viewed as content. Tunneling is the foundation for VPNs, which utilize public communication networks to connect private nodes. In VPNs, although information is passing via the public network, the “call-identifying information” in the encapsulated packet is not available to the transport carrier. From the point of view of the public network, the VPN’s call-identifying information does not exist; the public network only reads the signaling information necessary to get the information to the other end of the VPN; there the call identifying information particular to the VPN can be read. The fact that VPN information may not be available within the public network is, in fact, a key security feature demanded by VPN users. However, the VPN information is available from the VPN service provider. Thus, for the government to obtain signaling information identifying calls within the VPN, it has to go to the entity operating the VPN, just as it would in the case of any other private network.

C. A Service Provider Specific Interpretation Of Call-Identifying Information Is Consistent With The CALEA’s Plain Language And Legislative Intent

The statutory language and legislative history of CALEA indicate that Congress intended the distinction between call-identifying information and content to be determined from the perspective of the particular telecommunications carrier upon which an interception order is served.

1. The Definition of “Call-Identifying Information” Includes “Direction”

According to the CALEA, call-identifying information is:

²¹ TIA Reply Comments at 14.

dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by the subscriber equipment, facility, or service of a telecommunications carrier that is the subject of a court order or lawful authorization.²²

The inclusion of the word “direction” and the use of the disjunctive “or” in this definition are crucial. In the case of calls that are forwarded, a given carrier may not know the ultimate origin or destination or termination of a call, but the carrier will know its direction (the direction it is coming from and/or the direction it is going to). So in the case of packet data, the carrier may not be able to read through the layers of signaling protocols to know the ultimate origin or direction or destination of a communication, but it will surely know its immediate direction (i.e., where it came from and where it is going next).

2. Carriers Are Only Required To Provide Call-Identifying Information That Is “Reasonably Available”

CALEA requires that a telecommunications carrier be capable of “expeditiously isolating and enabling the government to access call-identifying information that is reasonably available to the carrier.”²³ Although the term “reasonably available to the carrier” is necessarily ambiguous, it is a very apt description of what happens in a packet environment. If higher layers of the stack are treated by the carrier as content, then they are not “available” to the carrier to be disclosed in response to a pen register order.

What is eminently reasonable, however, is for telecommunications carriers to separate call-identifying information from content for the protocol layers for which the carriers are responsible. If a carrier is implementing certain layers, then it must, logically, be able to separate

²² CALEA, § 103(a)(2).

the signaling information from the content. Therefore, such call-identifying information would be “reasonably available” almost by definition.

This layer-oriented analysis allows for the only bright line distinction to determine whether call-identifying information is reasonably available. Other types of analysis would result in endless dispute, require constantly shifting standards as technology developed, and create an administrative nightmare for the Commission. Adopting a subjective standard would also put carriers on notice of their responsibilities.

3. The Legislative History Shows That Congress Looked at Call-Identifying Information from the Perspective of the Carrier

The section-by-section analysis in the Committee Report could not be clearer:

The term ‘call-identifying information’ means the dialing or signaling information generated that identifies the origin and destination or [sic] a wire or electronic communication placed to, or received by, the facility or service that is the subject of the court order or lawful authorization. For voice communications, this information is typically the electronic pulses, audio tones, or signaling messages that identify the numbers dialed or otherwise transmitted **for the purpose of routing calls through the telecommunications carrier’s network**. In pen register investigations, these pulses, tones, or messages identify the numbers dialed from the facility that is the subject of the court order or other lawful authorization. In trap and trace investigations, these are the incoming pulses, tones, or messages which identify the originating number of the facility from which the call was placed and which are captured when directed to the facility that is the subject of the court order or authorization. Other dialing tones that may be generated by the sender that are used to signal customer premises equipment of the recipient are not to be treated as call-identifying information.²⁴

²³ CALEA, § 102(2).

²⁴ House Report at 21. Emphasis added.

As the Committee Report explicitly states, call-identifying information is that information which the telecommunication carrier uses to route calls through its own network. This definition concurs completely with the results of a subjective OSI reference model analysis.

For example, if a carrier is only providing layer 1 service, then the only signaling information to be provided would be the actual numbers dialed. If the carrier is providing layer 3 service, then the signaling information directed to layer 3 would be considered call-identifying information, according to the Committee Report. Higher layers become the equivalent of "other dialing tones that may be generated by the sender."²⁵

The Committee Report also states that a carrier is responsible only for providing information that it controls. The Report states that, "the question of which communications are in a carrier's control will depend on the design of the service or feature at issue."²⁶ Applying the OSI reference model here, it is easy to see that a carrier is not in control of a communication that takes place above the top most layer at which the carrier provides services. The Report goes on to make the same point in another way:

If, for example, a forwarded call reaches the system of the subscriber's carrier, that carrier is responsible for isolating the communication for interception purposes. However, if an advanced intelligent network directs the communication to a different carrier, the subscriber's carrier only has the responsibility...to ensure that law enforcement can identify the new service provider handling the communication.²⁷

²⁵ *Id.*

²⁶ *Id.* at 22.

²⁷ *Id.*

The analogy to the OSI reference model is obvious. Congress' intention was that if a message is being transported across several service providers, the subject carrier need only be able to name the succeeding service providers. This is exactly the same result that CDT is urging for packet networks.

It is possible that, under a subjective OSI reference model analysis, law enforcement agencies may not be able to get all the information they might desire for an investigation from a single carrier. However, according to the Report, this is not a problem that CALEA was intended to solve. As the Committee wrote, "the bill is not intended to guarantee 'one-stop shopping' for law enforcement."²⁸ If a law enforcement agency desires more information, it has two options. Either it can obtain a content interception order for the subject carrier, or it can obtain a pen register order for the service provider that has the information sought. As we have explained, there will always be a service provider in the network which uses that data as signaling information.

D. With A Subjective Standard, Capturing And Separating Routing Information Are Feasible

It is understandably difficult for a telecommunications carrier to capture and parse the protocols of packets in layers that the carrier is not responsible for. CDT is not proposing that carriers be required to capture layers for which they are not responsible. Under CDT's proposal, carriers would only be responsible to capture packet protocols within the OSI reference model layers for which they are responsible.

²⁸ *Id.*

It follows that if a carrier is responsible for services at a particular layer, then that carrier has the capability of parsing the packet protocols at that layer. A carrier could not provide services at a layer and not be able to parse the protocols at that layer. Identifying and capturing specific packets associated with a particular subscriber poses different problems, but should not be a concern if the proposed subjective analysis is adopted. After all, it is very reasonable to assume that a telecommunications carrier would be able to identify the subscribers who are utilizing its services. Additionally, it would be surprising if a telecommunications carrier providing high layer packet switched services did not have sophisticated tools for network performance monitoring and/or troubleshooting that permitted specific subscribers to be identified and isolated.

Before the Commission are difficult questions regarding the application of CALEA to packet-mode communications. The issues involved are intricate, but not unsolvable. They are inextricably intertwined with the three interests the Commission is required to balance: law enforcement needs, privacy protection, and innovation. It is our position that a clear and sound analytic framework for resolving these questions emerges from the very architecture of networks. More importantly, the proposed analysis provides an excellent balance of the three competing interests.

Alternative solutions to these problems fail because they are not balanced. The FBI/DOJ propose that all packet data be provided to them and that they will separate the call-identifying information from the content at their discretion. While we do not doubt the sincerity and integrity of the FBI, the potential for abuse is real and very high. Such an outcome would entirely undermine the intent of Congress to increase privacy protections through CALEA. The second alternative is that telecommunications carriers create the capability to parse packet

protocols for all layers of the OSI reference model. This is not CDT's position, although some may have assumed that it is. Instead, it is our recommendation that carriers be required only to provide what they treat as call-identifying data.

CONCLUSION

In their reports on CALEA, the House and Senate Judiciary Committees both stated "the bill does not require reengineering of the Internet, nor does it impose prospectively functional requirements on the Internet."²⁹ The increasing deployment of packet technologies in the public switched telephone network, as well as the increasing use of the Internet for voice telephony, raise questions for the conduct of electronic surveillance. We believe that these questions can be answered in the context of CALEA, without sacrificing either privacy or the interests of law enforcement, and without requiring reengineering of the Internet. We have outlined here a process for applying CALEA to packet technologies, by which a carrier using packet technologies can provide law enforcement with the signaling information that the carrier uses to route communications, without disclosing the associated content in the absence of a judicial order authorizing the acquisition of content.

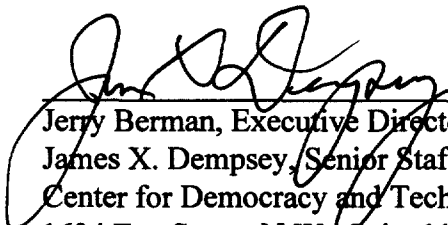
We also urge the Commission to reverse its tentative conclusion on location information. As we have shown, the Commission's *Further Notice* regarding location cannot be squared with the plain words of the statute. First, the word "location" does not appear in the definition of "call-identifying information." Second, each of the terms in the definition has a meaning independent of location. Third, Congress expressly stated "such call-identifying information

²⁹ *Id* at 23.

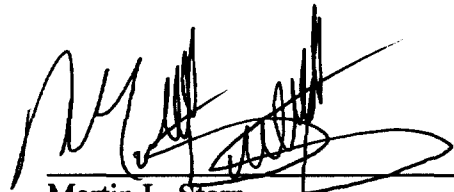
shall not include any information that may disclose the physical location of the subscriber." The Commission's effort to fit location into the terms of the Act produces a series of inconsistencies and illogical results. It is clear that the inclusion of location information in the industry J-STD was the result not of a reading of the statute's words, but rather of a desire by the industry to bring the standards negotiations to an end. The Commission's duty to adhere to the plain words of the statute requires it to reject a departure from the statute that prejudices the privacy rights of tens of millions of wireless phone users.

Respectfully submitted,

CENTER FOR DEMOCRACY AND TECHNOLOGY



Jerry Berman, Executive Director
James X. Dempsey, Senior Staff Counsel
Center for Democracy and Technology
1634 Eye Street, N.W., Suite 1100
Washington, D.C. 20006
(202) 637-9800
<http://www.cdt.org>



Martin L. Stern
Michael J. O'Neil
Preston Gates Ellis & Rouvelas
Meeds LLP
1735 New York Avenue, N.W., Suite 500
Washington, D.C. 20006
(202) 628-1700

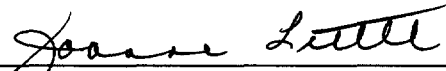
Attorneys for Center for Democracy and Technology

Of Counsel:
Ernest D. Miller, Law Student
Yale Law & Technology Society
Yale Law School
127 Wall Street
New Haven, CT 06520
<http://www.law.yale.edu/lawtech/>

Dated: December 14, 1998

CERTIFICATE OF SERVICE

I, Joanne Little, do hereby certify that copies of the foregoing Comments of the Center for Democracy and Technology have been served on the persons listed below on this 14th day of December, 1998.


Joanne Little

* BY HAND

*The Honorable William E. Kennard
Federal Communications Commission
1919 M Street, NW – Room 814
Washington, DC 20554

*The Honorable Harold Furchtgott-Roth
Federal Communications Commission
1919 M Street, NW – Room 802
Washington, DC 20554

*The Honorable Susan Ness
Federal Communications Commission
1919 M Street, NW – Room 832
Washington, DC 20554

*The Honorable Michael Powell
Federal Communications Commission
1919 M Street, NW – Room 844
Washington, DC 20554

*The Honorable Gloria Tristani
Federal Communications Commission
1919 M Street, NW – Room 826
Washington, DC 20554

*Gerald Vaughan, Acting Chief
Wireless Telecommunications Bureau
Federal Communications Commission
2025 M Street, NW – Room 5002
Washington, DC 20554

*David Wye
Telecommunications Policy Analyst
Wireless Telecommunications Bureau
Federal Communications Commission
2025 M Street, NW – Room 5002
Washington, DC 20554

*Dale Hatfield
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, NW – Room 230
Washington, DC 20554

***Charles Isman**

Office of Engineering and Technology
Federal Communications Commission
2000 M Street, NW – Room 230
Washington, DC 20554

***Paul Misener**

Federal Communications Commission
1919 M Street, NW – Room 802
Washington, DC 20554

***Peter A. Tenhula**

Federal Communications Commission
1919 M Street, NW – Room 844
Washington, DC 20554

***Magalie R. Salas**

Office of the Secretary
Federal Communications Commission
1919 M Street, NW – Room 222
Washington, DC 20554

***Tim Maguire**

Wireless Telecommunications Bureau
Federal Communications Commission
2100 M Street, NW – Room 8038
Washington, DC 20554

***David Sylvar**

Office of Engineering and Technology
Federal Communications Commission
2000 M Street, NW – Room 230
Washington, DC 20554

***Lawrence Petak**

Office of Engineering and Technology
Federal Communications Commission
2000 M Street, NW – Room 230
Washington, DC 20554

***Jim Burtle**

Office of Engineering and Technology
Federal Communications Commission
2000 M Street, NW – Room 230
Washington, DC 20554

***Ari Fitzgerald**

Federal Communications Commission
1919 M Street, NW – Room 814
Washington, DC 20554

***Karen Gulick**

Federal Communications Commission
1919 M Street, NW – Room 826
Washington, DC 20554

***Daniel Connors**

Federal Communications Commission
1919 M Street, NW – Room 832
Washington, DC 20554

***ITS**

1231 20th Street, NW
Washington, DC 20036

***Kimberly Parker**

Wireless Telecommunications Bureau
Federal Communications Commission
2100 M Street, NW – 7th Floor
Washington, DC 20554

***Rebecca Dorch**

Office of Engineering and Technology
Federal Communications Commission
2000 M Street, NW – Room 230
Washington, DC 20554